# Digital safety: A 30-minute tune-up

## What is the risk?

When you report on extremist groups, even if threats to your physical safety feel remote (and we shouldn't discount those either), the most likely type of risk is that you or your family members could get doxxed. This could include posting of private information like your home address, phone number, photos of your kids, attempts to access your bank accounts, etc. Another risk is that you could lose control of social media accounts, which hackers could use to post terrible things under your name.

These risks don't just apply to the people at the center of a story, or our public faces like anchors and radio hosts. If we're talking about doxxing, attackers may try to go after softer targets like your family members if they don't think they can intimidate you.

If we're talking about hacking, attackers will attempt to find weak links in an organization, then try to expand their access from there. It's critical that everyone in every news organization practices good password hygiene and uses 2-factor authentication for all digital services.

## In general:

-Do you use unique passwords or the same one over and over again? Make your important accounts (banks, credit cards, bills, social media) unique so if someone gains access to one account they can't get into everything.

-Never email passwords. Never ever. Delete any that are in your inbox or Trash.

-Set up professional social media accounts that are separate from your personal accounts.

## Gmail:

-Turn on 2-factor, use the authenticator app rather than SMS.
-Consider cleaning out old posts that include personal information, passwords, banking info, etc.
-Do this for your personal Gmail too!

## Facebook:

-Set up a professional page or account that is separate to your personal account.
-Turn on 2-factor authentication, use authenticator rather than SMS.
-Change your profile photo so it’s just you (or something generic) rather than a family member.
- Remove family members (or anybody else you don’t want everyone to see) from your “featured photos” which people can see even if your account is locked down tight.
-Do a “privacy checkup”
-On your phone, go to “Settings & Privacy”
-Click “Privacy Shortcuts”
-Go through:
-”Review a few important privacy settings”
-”See more privacy settings”
-”How People Find and Contact You”
-Optional and consequential: “Limit who can see past posts”
-After you're done, open an incognito window and search for yourself on Facebook. Are you OK with the world seeing what you can find?
-On your phone, find your profile, then click on “View As” to see what Facebook users who are not your friend can see.

## Twitter

-Turn on 2-factor, use the app version rather than SMS
-Change your profile photo as per above

## Instagram

-Head to “settings” (go to your profile, then the three-line drop down in the top right)
-Go to “security.”
-Turn on two-factor
-Go to “Privacy”
-Under “account privacy,” toggle to “private” if you’re public (unless you want anyone who finds your handle to see all your posts)
-Go to “tags”
-turn off “add automatically”
-you can also manually de-tag yourself from any photos others took. To do that, go to “hide photos and videos of you,” and check the photos you want hidden. This is particularly important if these photos contain friends who might not be private, or location tags, or if the photos themselves contain identifying info such as home addresses or license plates, etc.
-Go to “activity status”
-Turn off “activity status”

## Slack

-2-factor

## Doxx yourself/Remove public listings

One of the best ways to find privacy threats is to turn your reporting skills on yourself.

Google yourself and your home state, for example. What can you find? If you have not opted out of people search sites, you will find a lot you do not want public.

Here's how to opt out of several popular services that post a lot of personal info.

**FamilyTreeNow.com:**
https://www.familytreenow.com/optout

**Whitepages.com:**
https://support.whitepages.com/hc/en-us/articles/115010106908-How-do-I-edit-or-remove-a-personal-listing-

**Spokeo:**
https://www.spokeo.com/optout

**PeekYou:**
https://www.peekyou.com/about/contact/optout/

**InstantCheckmate.com:**
https://www.instantcheckmate.com/opt-out/

**Been Verified:**
https://support.beenverified.com/hc/en-us/articles/222411908-How-do-I-remove-my-name-from-BeenVerified-s-people-search-results-

# What to do if you suspect you have been hacked or doxxed:

If you suspect you've been doxxed (or had any other security incident occur) notify your manager or editor ASAP. If you think your email has been compromised, use another method of communication for this (Signal, walking over to them, etc.)

Investigation and mitigation resources;

https://www.rsaconference.com/writable/presentations/file_upload/hum-t19_hum-t19.pdf
http://www.cs.tufts.edu/comp/116/archive/fall2016/jmoyer.pdf
https://www.wired.com/story/what-do-to-if-you-are-being-doxed/
https://heimdalsecurity.com/blog/doxxing/
https://www.dhs.gov/sites/default/files/publications/How%20to%20Prevent%20Online%20Harrassment%20From%20Doxxing.pdf

## More tips, from the Committee to Protect Journalists:

https://cpj.org/2018/11/digital-safety-protecting-against-online-harassmen.php